

The Location Privacy Protection Act of 2011 (S. 1223)

Bill Summary

In January 2009, a special report by the Department of Justice revealed that approximately 26,000 persons are victims of GPS stalking annually, including by cellphone.

In December 2010, an investigation by the *Wall Street Journal* revealed that of 101 top apps for Apple iPhones and Google Android smartphones, 47 disclosed a user's location to third parties without his or her consent.

In April 2011, consumers learned that their Apple iPhone and Google Android smartphones were automatically sending Apple and Google information about the smartphone's whereabouts—even when users were not using location applications and, in Apple's case, even though users had no way to stop this collection.

These events have raised serious concerns among the American public about their location privacy on cellphones and smartphones. What most Americans still don't know is this: **Current federal laws allow many of the companies that obtain location information from their customers' cellphones and smartphones to give that information to almost anyone they please—without their customers' consent.** While the Cable Act and the Communications Act prohibit cable companies and phone companies offering telephone service from freely disclosing their customers' whereabouts, an obscure section of the Electronic Communications Privacy Act (18 U.S.C. § 2702) allows smartphone companies, app companies, and even phone companies offering wireless Internet service to freely share their customers' location information with third parties without first obtaining their consent.

This legal landscape creates a confusing hodgepodge of regulation. Thus, when a person uses a smartphone to place a phone call to a business, that person's wireless company can't disclose his location information to third parties without first getting his express consent. But when that *same* person uses that *same* phone to look up that business on the Internet, because of ECPA, his wireless company is legally free to disclose his location to anyone other than the government.

The Location Privacy Protection Act of 2011 (S. 1223), sponsored by **Senator Al Franken (D-MN)** and co-sponsored by **Senator Richard Blumenthal (D-CT)** is a narrowly-tailored bill that would close current loopholes in federal law to require any company that may obtain a customer's location information from his or her smartphone or other mobile device to (1) get that customer's express consent before collecting his or her location data; and (2) get that customer's express consent before sharing his or her location data with third parties.

The bill also (3) calls upon the National Institute of Justice to issue a study on the use of location technology in dating violence, stalking and domestic violence; (4) facilitates the reporting of these crimes to the FBI's Internet Crime Complaint Center; and (5) calls upon the Attorney General to develop a training curriculum so that law enforcement, courts, and victims advocates can better investigate and prosecute crimes involving the misuse of geo-location data. Finally, the bill puts up narrowly-constructed criminal penalties for the worst abusers of location technology. It (6) creates criminal penalties for so-called "stalking apps" that knowingly and intentionally disclose geolocation information while knowing and intending that domestic violence or stalking will occur as a result of this disclosure; and (7) criminalizes the knowing and intentional aggregation and sale of the location data of children 10 years old and younger.

The bill has the support of a broad coalition of consumer protection and anti-stalking advocacy groups.

*To co-sponsor the Location Privacy Protection Act of 2011 (S. 1223),
or for more information, contact Alvaro Bedoya at (202) 224-1024.*